REMARKS/ARGUMENTS

Prior to the entry of this Amendment, claims 1, 7, 9-14, 16, 20-25, 27, 31-36, and 53-57 were pending in this application. Claims 1, 16, and 27 have been amended, no claims have been canceled, and no claims have been added herein. Therefore, claims 1, 7, 9-14, 16, 20-25, 27, 31-36, and 53-57 are now pending in this application. Applicants request reconsideration of these claims for at least the reasons presented below.

Interview Summary

As an initial matter, the undersigned counsel thanks Examiner Teslovich for the professionalism and courtesy shown during the telephonic interview conducted between the undersigned and the Examiner on March 7, 2011. During that interview, the parties discussed possible claim amendments to highlight the distinctions between the reference relied upon in the current rejection and the pending claims. Such amendments as discussed in the interview have been made herein to highlight certain features of the invention. In summary, the Applicants contend that the references relied upon to date do not anticipate or render obvious the pending claims since none of them seem to suggest workflows for performing certificate related actions that affect the validity of a certificate, such as issuance, renewal, or revocation of the certificate, and that treat different users differently, i.e., requiring approval for some but not for others, based on the user's type, domain, etc. as recited in each independent claim. The amendments made herein, and the distinctions between the reference and the pending claims as discussed in the Interview are addressed in greater detail below.

Additionally, the Examiner introduced "Security Considerations for Workflow Systems" by Kittel et al. (herein after "Kittel") as potentially relevant to the pending claims. The Applicants respectfully contend that Kittel also would not anticipate or render obvious the pending claims. While the pending claims are not currently rejected based on Kittel, this reference will also be addressed in detail below in order to obviate any such rejection and to expedite prosecution of this application.

35 U.S.C. § 102 Rejection, Win

The Office Action rejected claims 1, 7, 9-14, 16, 20-25, 27, 31-36, and 53-57 under 35 U.S.C. § 102(e) as being anticipated by U. S. Patent No. 6,161,139 to Win et al. (hereinafter "Win"). The Applicants respectfully submit the following arguments pointing out significant differences between claims 1, 7, 9-14, 16, 20-25, 27, 31-36, and 53-57 submitted by the Applicants and Win.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP 2131 citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Applicants respectfully argue that Win fails to disclose each and every claimed element. For example, Win fails to disclose, either expressly or inherently, workflows for performing certificate related actions that affect the validity of a certificate, such as issuance, renewal, or revocation of the certificate, and that treat different users differently, i.e., requiring approval for some but not for others, based on the user's type, domain, etc. as recited in the pending claim.

Win is directed to "managing and administering, from several distributed locations, a system for facilitating secure and selective access to network resources based on a role of a user of the resources." (Col. 1, lines 21-24) More specifically, Win describes "delegating to a user the administration of an access control computer system." (Col. 2, lines 55-56) Under Win:

> "The method comprises storing information that defines administration roles, that associates a user with one or more of the administrative roles, and that associates each administration role with one or more administrative privileges. An administrative privilege authorizes at least one administrative function. When the user requests the execution of an administrative function, the requests is honored only when one of the user's administrative roles includes an administrative privilege that authorizes the requested administrative function." (Col. 2, lines 55-65)

That is, Win describes delegating administrative tasks to different user and, while Win may describe relying on certificates for authentication of users, Win does not address processes for affecting the validity of those certificates (i.e., issuance, revocation, renewal). Thus, Win cannot be read to disclose, expressly or inherently, workflows for performing certificate related actions that affect the validity of a certificate, such as issuance, renewal, or revocation of the certificate, and that treat different users differently, i.e., requiring approval for some but not for others, based on the user's type, domain, etc. as recited in the pending claims. For at least these reasons, the Applicants respectfully request withdrawal of the rejection.

Kittel

As noted above, during the Interview the Examiner introduced Kittel as potentially relevant to the pending claims. While the pending claims are not currently rejected based on Kittel, this reference is addressed here in order to obviate any such rejection and to expedite prosecution of this application. More specifically, the Applicants respectfully contend that Kittel also would not anticipate or render obvious the pending claims for at least the following reasons.

Kittel is directed to security issues facing a workflow system (such as an OSS) and ways to provide security to that system such as through a model that uses the secure socket layer protocol and HTTPS tunneling mechanism. (See for example Abstract) As noted in Kittel "what secure e-business systems (including secure workflow systems) really need is an integrated security infrastructure that can offer such services as authorization, authentication, access control, data confidentiality, data integrity, auditing, non-repudiation, and security management and administration." (Section 1. Introduction, second paragraph) To this end, Kittel describes a set of interfaces (i.e., APIs) for workflow engines that provide a set of functions through which systems direct activities to various components and on which security functions such as authentication and access control can be applied. (See for example Section 2.1 Workflow Systems Interfaces)

However, Kittel does not disclose, expressly or inherently and would not teach or suggest, alone or in combination with Win, workflows for performing certificate related actions that affect the validity of a certificate, such as issuance, renewal, or revocation of the certificate, and that treat different users differently, i.e., requiring approval for some but not for others, based on the user's type, domain, etc. as recited in the pending claims. Rather, Kittel may suggest utilizing certificates within a workflow system, such as to authenticate a user (see for example Section 2.3 Security Level and Policy-based Security Management) but does not seem to address issuance, renewal, revocation or anything else that effects the validity of those certificates and, more specifically, does not suggest workflows that do so and that distinguish between users (requiring some to obtain approval and other not) based on a user's type, domain, etc. For at least these reasons, Kittel would not seem to form a basis for a proper rejection of the pending claims.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

/William J. Daley/
William J. Daley
Reg. No. 52,471

KILPATRICK TOWNSEND & STOCKTON LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000 (Denver office)
Fax: 303-571-4321 (Denver office)
WJD:jep

63128110 v1